Tampereen ammattikorkeakoulu

Pilvipalveluiden turvallisuus ja saatavuus

Jussi Latva-Mäenpää

OPINNÄYTETYÖ
Huhtikuu 2023

Tietotekniikan tutkinto-ohjelma
Tietoliikennetekniikka ja tietoverkot

TIIVISTELMÄ

Tampereen ammattikorkeakoulu
Tietotekniikan tutkinto-ohjelma
Tietoliikennetekniikka ja tietoverkot

LATVA-MÄENPÄÄ, JUSSI:
Pilvipalveluiden turvallisuus ja saatavuus

Opinnäytetyö 24 sivua, joista liitteitä 2 sivua
Huhtikuu 2023

Opinnäytetyössä kerrotaan, mitä pilvipalvelut ovat, sekä käydään läpi yleisimmät pilvipalvelu- ja toteutusmallit. Työssä selvennetään pilvipalvelu- ja toteutusmallien käyttökohteita ja tutustutaan kunkin mallin vahvuuksiin ja haavoittuvuuksiin. Työn tavoitteena oli tutkia pilvipalveluiden tarjontaa maailmanlaajuisesti sekä perehtyä pilvipalveluiden tietoturvaan pilvipalveluiden turvallisuuden arviointikriteeristön avulla. Tämän lisäksi opinnäytetyö kertoo pilvipalveluiden käyttöasteesta suomalaisissa yrityksissä. Työ toteutettiin internetartikkeleihin sekä teknisiin dokumentaatioihin perustuvana kirjallisuuskatsauksena.

Opinnäytetyöstä selviää, että suomalaiset suuret toimijat pääsääntöisesti käyttävät maailmanlaajuisesti suuria pilvipalveluiden tarjoajia. Työssä kuvataan myös, kuinka yritysten ja käyttäjien tulisi varautua ja reagoida eri uhkiin ja riskeihin.

Pilvipalveluiden käyttö on viime vuosien aikana kasvanut roimasti, mutta kotimainen pilvipalveluiden tarjonta on vielä maailmanlaajuisesti suurien tarjoajien varjossa. Pilvipalveluiden tietoturvaan on palveluiden käytön lisääntymisen yhteydessä alettu kiinnittää enemmän huomiota. Hyvä työkalu yrityksille pilvipalveluiden tietoturvan kehittämiseen on vuonna 2020 Kyberturvallisuuskeskuksen laatima pilvipalveluiden turvallisuuden arviointikriteeristö, josta löytyy varmasti kehittämisehdotuksia niin suurille kuin pienillekin yrityksille.

Asiasanat: tietoturva, saatavuus, pilvipalvelu

ABSTRACT

Tampereen ammattikorkeakoulu
Tampere University of Applied Sciences
Degree Programme in ICT Engineering
Telecommunications and Networks

LATVA-MÄENPÄÄ, JUSSI:
Safety and availability of cloud services

Bachelor's thesis 24 pages, appendices 2 pages
April 2023

This thesis clarified what cloud services are and went through the most common cloud service and deployment models. The thesis also introduced some use cases for each cloud service and deployment model and showcased the strengths and weaknesses of each model. The main goal of the thesis was to study the biggest cloud service providers globally and to explore data security of cloud services using the criteria by National Cyber Security Center. In addition, the thesis told about the usage rate of the cloud services in Finnish companies. This study was carried out as a literature review using an assortment of internet articles and technical documents.

The thesis explained how large Finnish companies generally use global cloud service providers. The thesis also explained how companies and users should prepare and react to different data security threats and risks.

Usage of the cloud services has rapidly increased in only a few years, but Finnish cloud service providers are still in the shadow of global providers, even amongst Finnish customers. With the increase of cloud service usage, more attention has started to be paid to the information security of cloud services. A great tool for companies to develop their information security is the evaluation criteria for the security of cloud services, which was prepared by the Finnish National Cyber Security Centre in 2020.

Key words: information security, availability, cloud service

SISÄLLYS

LYHENTEET JA TERMIT

AWS	Amazon Web Services on Amazon.com:in tarjoama pilvipalvelu
CaaS	Containers as a Service on pilvipalvelumalli, jossa käyttäjä voi ajaa omia konttejaan
FaaS	Function as a Service on pilvipalvelumalli, joka
GCP	Google Cloud Platform on Alphabet Inc.:in tarjoama pilvipalvelu
IaaS	Infrastructure as a Service on pilvipalvelumalli, jossa fyysinen laitteisto on palveluntarjoajan vastuulla
PaaS	Platform as a Service on pilvipalvelumalli, joka tarkoittaa kehitys- ja julkaisualustaa pilvessä
PiTuKri	Traficomin sekä kyberturvallisuuskeskuksen luoma pilvipalveluiden turvallisuuden arviointikriteeristö
SaaS	Software as a Service on pilvipalvelumalli, joka tarkoittaa ohjelmistoa pilvipalveluna

1 JOHDANTO

Yritysten digitalisoituminen vauhdittui koronapandemian myötä huomattavasti, sillä yritykset joutuivat nopealla aikataululla siirtyä esimerkiksi etätyöskentelyyn, sekä ottamaan käyttöön erinäisiä pilvipalveluita. Suuressa osassa yrityksistä termillä tarkoitetaan sähköpostipalveluita tai perinteistä pilvitallennustilaa kuten OneDrive tai Dropbox, mutta todellisuudessa käsite sisältää paljon enemmän käyttötarkoituksia. Esimerkkinä pilvessä voidaan suorittaa erinäisiä ohjelmia etänä tai ylläpitää yritysten tietokantoja.

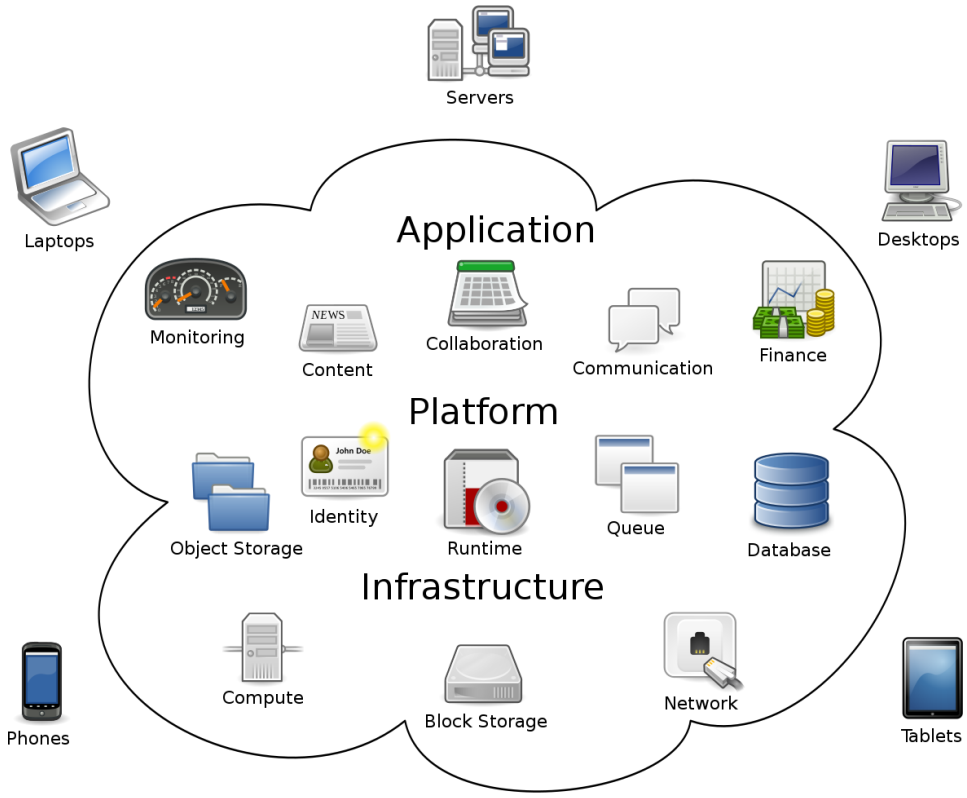
Tämän nopean digitalisoitumisen myötä myös huoli pilvipalveluiden tietoturvasta on kasvanut. Tässä opinnäytetyössä pyrin selkeyden vuoksi ensin käymään läpi erilaiset pilvipalvelumallit ja toteutusmallit, tarkastelemaan pilvipalveluiden tarjontaa opinnäytetyön tekemisen hetkellä sekä tarkastelemaan pilvipalveluihin mahdollisesti kohdistuvia uhkia ja tietoturvaratkaisuja.

2 PILVIPALVELUT

Ennen syvempää perehtymistä pilvipalveluiden tietoturvaan sekä saatavuuteen, on tärkeää tietää mitä pilvipalvelut ovat.

2.1 Mitä ovat pilvipalvelut?

Pilvipalvelut ovat joukko IT-sovelluksia ja resursseja, jotka sisältävät ohjelmistoja, infrastruktuuria ja alustoja (kuva 1), joita isännöivät kolmannen osapuolen palveluntarjoajat ja joita toimitetaan sopimuksen mukaan organisaatioille, yrityksille sekä yksittäisille asiakkaille internetin välityksellä (Cloud Services. Corporate Financial Institute, 2023). Toimivat pilvipalvelut rakennetaankin aina asiakkaan tarpeiden ja tavoitteiden pohjalta. Pilvipalvelut luovat tärkeitä etuja kuten skaalautuvuuden tarpeen ja käytön mukaan, mikä taas lisää palvelun kustannustehokkuutta ja käyttömahdollisuuksia. (Liimatta, 2021.)

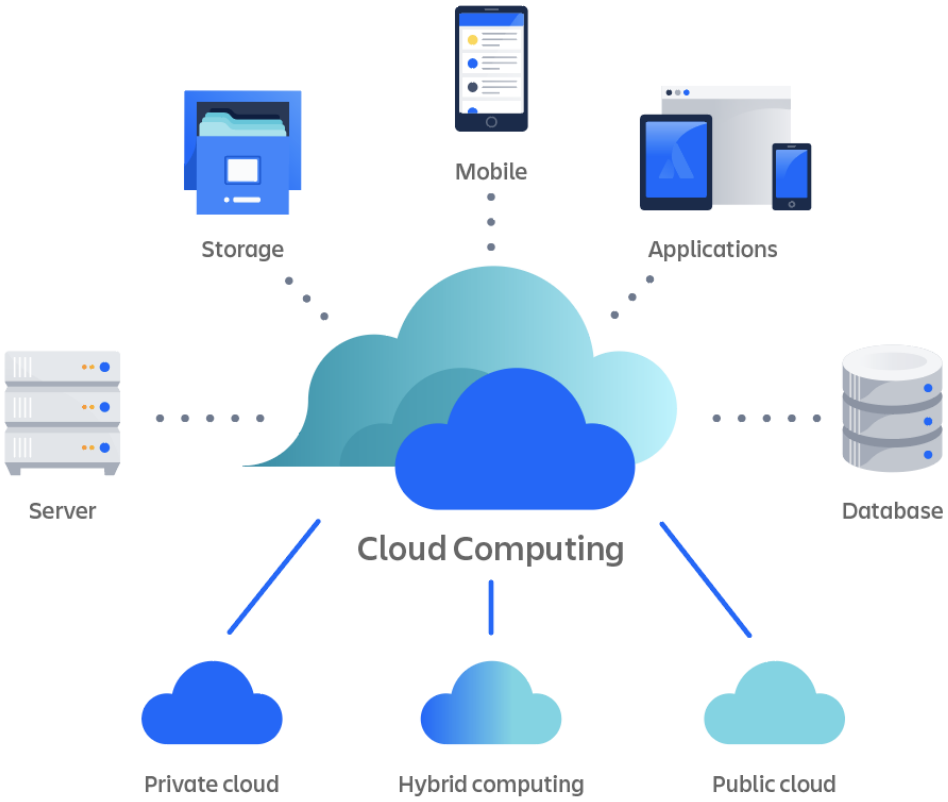


KUVA 1. Esimerkkikuva pilvipalveluiden mahdollisista käyttökohteista (Johnston, 2009).

2.2 Toteutusmallit

Pilvipalveluilla on kolme pääsääntöistä toteutusmallia, joista jokaisella on omat vahvuutensa. Organisaatiot usein hyötyvätkin useasta eri toteutusmallista (Zettler N.d.).

- Yksityinen pilvi (Private cloud)
- Julkinen pilvi (Public cloud)
- Hybridipilvi (Hybrid cloud)



KUVA 2. Esimerkkikuva pilvipalveluiden toteutusmalleista (Zettler N.d.).

2.2.1 Yksityinen pilvi

Yksityinen pilvi on toteutusmalli, joka kuuluu vain yhdelle yritykselle tai organisaatiolle. Se sijaitsee kyseisen yrityksen tai organisaation omassa yksityisessä

verkossa. Tämä toteutusmalli on yleensä käytössä rahoitusalalla, julkisella sektorilla sekä joissain keskisuurissa ja monissa suurissa organisaatioissa (Liimatta, 2021).

IT-infrastruktuuriin tarvitaan yritykseltä tai organisaatiolta huomattavia investointeja, jotta pystytään rakentamaan oma datakeskus ja asentamaan sinne tarvittavat laitteistot ja ohjelmistot yksityistä pilveä varten (Cloud Services. Corporate Financial Institute, 2023.) Tämä prosessi on myös mahdollista ulkoistaa IT-kumppanille.

Yksityinen pilvi on omiaan korkeamman turvatason palveluita varten. Sen vahvuutena on pilvipalveluinfrastruktuurin ja käsiteltävien tietojen sekä loogisen tason luotettava erottelu muista organisaatioista, ulkoisista toimijoista sekä muista tietojenkäsittely-ympäristöistä (Pilvipalveluiden turvallisuuden arviointikriteeristö, 2020).

2.2.2 Julkinen pilvi

Julkinen pilvi on toteutusmalli, jonka avulla toimitetaan resursseja kuten sovelluksia, tallennustilaa, palvelimia sekä esimerkiksi laskentaresursseja internetin välityksellä. Tässä toteutusmallissa palveluntarjoaja omistaa ja hallinnoi kaikkia laitteita, ohjelmistoja sekä muita infrastruktuureja, joita pilvipalveluiden toimittamiseen liittyy. (Zettler N.d.)

Julkisessa pilvessä käsiteltäviin tietoihin muodostuu suurempi hyökkäyspinta-ala palvelun muiden käyttäjien sekä toisten toimijoiden kautta (Pilvipalveluiden turvallisuuden arviointikriteeristö, 2020). Esimerkkejä julkisen pilven palveluntarjoajista ovat mm. IBM, Microsoft Azure, Amazon Web Services (AWS) ja Google Cloud Platform (GCP) (Liimatta, 2021).

2.2.3 Hybridipilvi

Hybridipilvi on toteutusmalli, joka on nimensä mukaisesti yhdistelmä yksityistä ja julkista pilveä. Ne ovat yhdistetty teknologiaan, joka sallii eri toteutusmallien yhteistyön. Käyttökohteena tälle toteutusmallille on arkaluontoisten tietojen ja palveluiden säilyttäminen suojatussa yksityisessä pilvessä, kun taas julkisesti saatavilla olevat verkkopalvelimet sekä asiakaslähtöiset päätepisteet voivat elää julkisessa pilvessä. (Zettler N.d.). Yhdistelmäpilvessä toteutuvan turvallisuuden taso riippuu paljon siitä, minkälaisia tietoja on mahdollista siirtyä yksityisestä pilvestä julkiseen pilveen, sekä siitä miten tietoturva on toteutettu pilvien rajapinnassa (Pilvipalveluiden turvallisuuden arviointikriteeristö, 2020).

2.3 Pilvipalvelumallit

Pilvipalveluihin sisältyy monia erilaisia pilvipalvelumalleja, joita on alettu erittelemään käyttämällä X-as-a-Service -käsitettä. Seuraavassa kappaleessa perehdytään viiteen eri XaaS -käsitteeseen ja esitellään näille eri käyttökohteita. Kuvassa 3 verrataan eri XaaS -käsitteitä ja näiden tarjoamien palveluiden hallinnointisuhteita yrityksen omaan konesaliin verrattuna.

KUVA 3. Pilvipalvelumallit verrattuna oman konesalin ylläpitämiseen. (Vento, 2020).

2.3.1 Infrastructure as a Service (IaaS)

IaaS eli Infrastructure as a Service on pilvipalvelumalli, jossa fyysinen laitteisto ja sen ylläpito, sekä virtualisointi on palveluntarjoajan vastuulla. Käyttökohteena IaaS -palveluille yleensä ovat konttipalvelut sekä virtuaalikoneet. Asiakkaan vastuulle jää esimerkiksi verkon konfigurointi, sekä virtuaalikoneiden tai konttien ajaminen. (Vento, 2020).

2.3.2 Platform as a Service (PaaS)

PaaS eli Platform as a Service on pilvipalvelumalli, joka tarkoittaa kehitys- ja julkaisualustaa pilvessä (Vento, 2020). PaaS sisältää infrastruktuurin IaaS tavoin, mutta sen lisäksi PaaS voi sisältää esimerkiksi väliohjelmistoja, kehitystyökaluja sekä tietokannan hallintajärjestelmiä. (What is PaaS? Microsoft Azure, 2023).

2.3.3 Function as a Service (FaaS)

FaaS eli Function as a Service on pilvipalvelumalli, joka tarkoittaa alustaa funktioiden ajamiselle. Puhuttaessa palveliton-arkkitehtuurista (serverless-architecture) tarkoitetaankin yleensä FaaS -palveluita. FaaS -palvelut ovat omiaan suorittamaan funktioita, joita tarvitsee suorittaa vain tietyin väliajoin. Palveluntarjoaja voi suorittaa funktion pyynnöstä, jolloin funktiota varten ei tarvitse perustaa omaa palvelinta (Vento, 2020).

2.3.4 Containers as a Service (CaaS)

CaaS eli Containers as a Service tarkoittaa pelkistettynä pilvipalvelua, jossa käyttäjä voi ajaa omia konttejaan palveluntarjoajan tarjoamassa infrastruktuurissa. (Vento, 2020).

2.3.5 Software as a service (SaaS)

SaaS eli Software as a Service tarkoittaa ohjelmistoa pilvipalveluna. Hyviä esimerkkejä tästä ovat Office 365 ja Gmail (Vento, 2020). Käytännössä palveluntarjoaja tarjoaa ohjelmiston kokonaisuudessaan, jolloin asiakas vain käyttää tätä palvelua internetin välityksellä.

3 PILVIPALVELUIDEN TARJONTA

Vuoden 2022 keväällä maksullisia pilvipalveluita käytti 81 % yrityksistä. Kahdeksassa vuodessa tämä tilasto on kasvanut 30 prosenttiyksikköä (Liite 1). Tämän kasvun myötä myös pilvipalveluiden tarjonta on lisääntynyt.

3.1 Maailmanlaajuisesti suurimmat pilvipalveluiden tarjoajat

Suurimmat pilvipalveluntarjoajat ovat tuoneet muutoksia IT-infrastruktuurin markkinoille maailmanlaajuisesti. On siis hyvä tuntea johtavat pilvipalveluiden tarjoajat, sekä näiden eriävät strategiat (Zhang, 2023).

Tässä työssä perehdymme kolmeen suurimpaan pilvipalveluiden tarjoajaan.

Maailmanlaajuisesti suurimmat pilvipalveluiden tarjoajat:

- Amazon Web Services (AWS)
- Microsoft Azure
- Google Cloud Platform (GCP)
- Alibaba Cloud
- Oracle Cloud
- IBM Cloud (Kyndryl)
- Tencent Cloud
- OVHcloud
- DigitalOcean
- Linode (Akamai)

(Top 10 Cloud Service Providers Globally in 2023)

3.1.1 Amazon Web Services (AWS)

Amazon Web Services on Amazon.com:in tarjoama pilvipalvelu. AWS on tällä hetkellä suurin pilvipalveluiden tarjoaja, ja se sisältää sekoituksen IaaS, PaaS sekä SaaS tarjontaa.

AWS tarjoaa yli 200 täysin varusteltua palvelua, mukaan lukien laskenta-, tallennus- ja tietokantapalveluita (Zhang, 2023). Jokainen palvelu voidaan myös konfiguroida eri tavoin käyttäjän tarpeiden mukaan (Barney & Gillis, 2022).

AWS:llä on tällä hetkellä toiminnassa 26 aluetta (region) ja 84 saatavuusaluetta (availability zone). Nämä alueet ja saatavuusalueet sijaitsevat Yhdysvalloissa, Etelä-Amerikassa, Euroopassa, Aasian ja Tyynenmeren alueella sekä Lähi-idässä ja Afrikassa. (Zhang, 2023.)

3.1.2 Microsoft Azure

Microsoft Azure on Microsoft Corporationin tarjoama pilvipalvelu. Microsoft Azure on tällä hetkellä toiseksi suurin pilvipalveluiden tarjoaja maailmanlaajuisesti. Microsoft Azure tarjoaa asiakkailleen yhtenäisen hybridipilvikokemuksen. (Zhang, 2023.)

Microsoft Azurella on tällä hetkellä toiminnassa 60 aluetta ja 116 saatavuusaluetta. Nämä alueet ja saatavuusalueet sijaitsevat Yhdysvalloissa, Etelä-Amerikassa, Euroopassa, Aasian ja Tyynenmeren alueella sekä Lähi-idässä ja Afrikassa. (Zhang, 2023.)

Microsoftilla on maailmanlaajuisesti yli 200 fyysistä Microsoft Azure datakeskusta. Niitä yhdistää yli 280000 kilometriä kuitulinjoja 140 maassa. (Zhang, 2023.)

3.1.3 Google Cloud Platform (GCP)

Google Cloud Platform on Alphabet Inc.:in tarjoama pilvipalvelu, joka on tällä hetkellä maailmanlaajuisesti kolmanneksi suurin pilvipalveluiden tarjoaja. Google Cloud Platform tarjoaa skaalautuvan infrastruktuurin yrityksille, jonka avulla kehittäjät voivat rakentaa, testata sekä ottaa käyttöön sovelluksia, samalla hyödyn-

täen palvelun turvallisuuden, tiedonhallinnan analytiikan sekä tekoälyn ominaisuuksia (Zhang, 2023). Vuonna 2023 Google Cloud Platform toi uudet generatiiviset tekoälyominaisuudet kuten Vertex AI:n sekä Generative AI App Builderin Google Cloudiin (Kurian, 2023).

Google Cloud Platformilla on tällä hetkellä toiminnassa 34 aluetta ja 103 saatavuusaluetta. Nämä alueet ja saatavuusalueet sijaitsevat Yhdysvalloissa, Etelä-Amerikassa, Euroopassa sekä Aasian ja Tyynenmeren alueella. (Zhang, 2023.)

3.2 Suomalaiset pilvipalveluiden tarjoajat

Tässä opinnäytetyössä suomalaisena pilvipalveluiden tarjoajana pidetään sellaista yritystä, jonka konesalit sijaitsevat Suomessa. Suomalaisista pilvipalveluista on mahdotonta tällä hetkellä päätellä käyttöastetta, sillä tutkimusta palveluiden yleisyydestä ei ole tehty.

Tällaisia yrityksiä ovat ainakin:

- Kaita
- Otaverkko
- Netox
- Easy Pilvipalvelin (Tietopalvelut Group)

Kaikki yllä mainituista yrityksistä mainitsevat verkkosivuillaan konesalien sijaitsevan Suomessa, sekä noudattavan ISO (International Organization for Standardization) 27001-sertifikaattia. Sertifikaatti käsittelee tietoturvallisuuden hallintajärjestelmän toteuttamista, ylläpitämistä sekä parantamista koskevia vaatimuksia. (Vetikko, 2019).

4 PILVIPALVELUIDEN TIETOTURVA

Pilvipalveluiden turvallisuus kokonaisuudessaan muodostuu sekä palveluntarjoajan että asiakkaan tietoturvakäytännöistä, sekä pilveen siirrettävän sovelluksen tietoturvasta (Pilvipalveluiden turvallisuus, 2014). Kyberturvallisuuskeskuksen ja Traficomin laatiman Pilvipalveluiden turvallisuuden arviointikriteeristön (PiTuKri) tavoitteena on edistää viranomaisten salassa pidettävän tiedon turvallisuutta tilanteissa, joissa tietoja käsitellään pilvipalveluissa (Pilvipalveluiden turvallisuuden arviointikriteeristö, 2020). Kriteeristö on myös hyvä työkalu yritysten sekä eri organisaatioiden käyttöön oman pilvipalveluinfrastruktuurin suunnittelua varten.

4.1 Pilvipalveluiden uhat ja riskit

Pilvipalveluiden turvallisuuden arviointikriteeristöstä selviää, että pilvipalveluihin kohdistuu uhkia ja riskejä niin teknisellä kuin ei-teknisellä tasolla.

Teknisen tason uhkiin ja riskeihin voi luokitella mm. seuraavia asioita:

- Yleiset verkkohyökkäykset
- Käyttöoikeuksien hallinnan puute
- Hallintayhteyksien haavoittuvuus
- Käyttäjien tunnistautuminen

Ei-teknisen tason uhkiin ja riskeihin voi luokitella mm. seuraavia asioita:

- Palveluntuottajat ja vierailijat
- Luvaton pääsy (fyysiseen sijaintiin)
- Heikot rakenteet ja/tai turvallisuusjärjestelmät (fyysisen sijainti)
- Henkilöstön luotettavuuden arvioinnin puute
- Käyttäjien turvallisuustietoisuus

(Pilvipalveluiden turvallisuuden arviointikriteeristö, 2020).

4.2 Henkilöstöturvallisuus

Henkilöstöturvallisuus on tietoturvan kulmakivi. On tärkeää, että ennen työsuhteen aloittamista työnantaja arvioi työntekijän luotettavuuden, sekä allekirjoittaa työntekijän kanssa mahdollisesti tarvittavat salassapito- ja vaitiolositoumukset.

4.2.1 Henkilöstön luotettavuuden arviointi

Niin sisäisten kuin ulkoisten työntekijöiden taustat tulee tarkastaa lainsäädännön mahdollistamien menettelyjen mukaisesti ennen kuin työsuhdetta aloitetaan, jos työntekijällä tulee olemaan pääsy pilvipalveluiden asiakkaiden tietoihin (Pilvipalveluiden turvallisuuden arviointikriteeristö, 2020).

Lainsäädännön sallimissa rajoissa tarkistuksen olisi hyvä sisältää:

- Henkilöllisyyden todentaminen
- Työhistorian todentaminen
- Koulutustaustan todentaminen

(Pilvipalveluiden turvallisuuden arviointikriteeristö, 2020).

4.2.2 Salassapito- ja vaitiolositoumukset

Ennen työnantajan ja työntekijän sopimussuhteen alkamista on kirjoitettava salassapitosopimukset, ennen kuin työntekijälle myönnetään pääsy pilvipalvelun asiakkaiden tietoihin. (Pilvipalveluiden turvallisuuden arviointikriteeristö, 2020).

4.2.3 Turvallisuustietoisuus

Turvallisuustietoisuus tarkoittaa sitä, että keskeiset turvallisuuteen liittyvät periaatteet ja toimintatavat ovat henkilöstölle ohjeistettuna, ne ovat ajan tasalla ja että näiden turvallisuusohjeiden noudattamista valvotaan (Pilvipalveluiden turvallisuuden arviointikriteeristö, 2020).

4.2.4 Tiedonsaantitarpeet ja tehtävien erottelu

Tiedonsaantitarpeet ja tehtävien erottelu tarkoittaa sitä, että salassa pidettävät tiedot päätyvät vain valtuutetuille henkilöille vain tarpeen niin vaatiessa. Tällä tavoin pienennetään salassa pidettävään tietoon kohdistuvia riskejä (Pilvipalveluiden turvallisuuden arviointikriteeristö, 2020).

4.2.5 Käyttäjätunnistus

Pilvipalvelun tuottamiseen liittyvät palveluntarjoajan ylläpitäjät, sekä asiakkaan ylläpitäjät ja palvelun käyttäjät täytyy todentaa luotettavasti ennen pääsyä suojattavaan tietoon. Käyttäjätunnistuksen tulisi täyttää seuraavat vaatimukset:

- Yksilölliset henkilökohtaiset käyttäjätunnisteet.
- Käyttäjätunnuksen tulee lukittua, jos tunnistus epäonnistuu liian monta kertaa peräkkäin.
- Käyttäjien todennus tulee tehdä vahvasti kaksivaiheisella tunnistautumisella.

(Pilvipalveluiden turvallisuuden arviointikriteeristö, 2020).

4.3 Fyysinen turvallisuus

Fyysisellä turvallisuudella viitataan pilvipalveluiden tuottajan tai hallitsijan konesalien rakenteisiin, turvallisuusjärjestelmiin sekä kulunvalvontaan (Pilvipalveluiden turvallisuuden arviointikriteeristö, 2020).

4.3.1 Rakenteet ja turvallisuusjärjestelmät

Kokonaisturvallisuuteen vaikuttaa paljon konesalin fyysinen sijainti. Varkauksien sekä vahinkojen minimoimiseksi konesalin tulee sijaita rakenteiltaan sekä turval-

lisuusjärjestelmiltään oikein suunnitellussa tilassa (Pilvipalveluiden turvallisuuden arviointikriteeristö, 2020). Kappaleessa 3.2 mainittu sertifikaatti ISO 27001 sisältää vaatimukset konesalin rakenteisiin liittyen.

4.3.2 Luvattoman pääsyn estäminen

On tärkeää, että pilvipalvelussa säilytettävään salattuun tietoon, sekä sitä käsiteltäviin laitteisiin tai näiden turvallisuudesta huolehtiviin järjestelmiin kuten palomuureihin on pääsy vain valituilla ja todennetuilla henkilöillä (Pilvipalveluiden turvallisuuden arviointikriteeristö, 2020).

4.4 Tietoliikenneturvallisuus

Olennaisena osana tietoliikennetuotetta on tietoliikenneturvallisuus. Tietoliikenneturvallisuudessa tulee huomioida vastuunjako asiakkaan sekä palveluntarjoajan välillä. Esimerkiksi IaaS-mallissa palveluntarjoaja ei pysty vaikuttamaan asiakkaan vastuulla olevien palomuurien tietoturvaan, kun taas asiakas ei pysty vaikuttamaan infrastruktuurialustan tietoturvaan. (Pilvipalveluiden turvallisuuden arviointikriteeristö, 2020).

4.4.1 Luvattoman pääsyn estäminen

Tietoliikenneverkon rakenteen on hyvä olla suunniteltu niin, että pilvipalveluympäristö on erotettu muista ympäristöistä. Liikennöinnin tulisi olla rajoitettu niin, että vain erikseen hyväksytty, toiminnalle välttämätön liikennöinti on sallittu pilvipalveluympäristön ulkoreunalla ja sisäisten alueiden välillä (Pilvipalveluiden turvallisuuden arviointikriteeristö, 2020).

4.4.2 Verkkohyökkäyksiä vastaan suojautuminen

Organisaation tulee ylläpitää riskienarviointia, joka kattaa myös verkkohyökkäyksiltä suojautumisen. Suojauksien tulisi olla suunniteltu niin, että hyökkäykset eivät vaaranna käsiteltävän tiedon tai palveluiden luottamuksellisuutta (Pilvipalveluiden turvallisuuden arviointikriteeristö, 2020).

5 POHDINTA

Opinnäytetyön tavoitteena oli selkeyttää pilvipalveluiden rakennetta esittelemällä erilaisia käytössä olevia pilvipalvelu- sekä toteutusmalleja, tarkastelemaan pilvipalveluiden tarjontaa suomessa sekä maailmanlaajuisesti, sekä tarkastelemaan pilvipalveluihin kohdistuvia uhkia ja näiden tietoturvaratkaisuja. Opinnäytetyön aiheen antoi Tampereen Ammattikorkeakoulu.

Opinnäytetyössä joutui nojautumaan suurelta osin englanninkieliseen materiaaliin, sillä aiheesta tehtyä suomenkielistä materiaalia oli hyvin vähän saatavilla. Jos suomenkielistä materiaalia oli saatavilla, niistä suurin osa oli erinäisten tietotekniikkayritysten edustajien kirjoittamia uutisia tai blogeja yritysten omilla verkkosivuilla.

Tärkein materiaali opinnäytetyötä tehdessäni oli kuitenkin suomenkielinen Traficomin sekä Kyberturvallisuuskeskuksen kirjoittama Pilvipalveluiden turvallisuuden arviointikriteeristö, joka käsittelee opinnäytetyössä suuressa osassa olevaa pilvipalveluiden tietoturvaa.

Opinnäytetyötä kirjoittaessa huomasin, että kotimaassa pilvipalveluiden suuret käyttäjät kuten eduskunta, käyttävät maailmanlaajuisestikin suuria pilvipalveluiden tarjoajia kuten Amazon Web Servicesiä. Suomalaisten pilvipalveluiden tarjoajien asiakaskuntaan olikin yllättävän vaikea perehtyä, sillä aiheesta ei löytynyt tutkimustietoa. Huomasin myös, että pilvipalveluiden käyttö on lisääntynyt huomattavasti, tilastokeskuksen mukaan vuonna 2014 pilvipalveluita käytti 51% yrityksistä, ja vuonna 2022 luku oli 81% (Liite 1).

Pilvipalvelut ovatkin nykyään todella tärkeä työkalu kaiken kokoisissa yrityksissä, juuri skaalautuvuutensa ja monipuolisuutensa vuoksi.

LÄHTEET

Cloud Services. Corporate Financial Institute. 2023. Verkkojulkaisu. Viitattu 3.4.2023. https://corporatefinanceinstitute.com/resources/data-science/cloud-services/

Liimatta, A. 2021. Pilvipalvelut: tiedä tärkeimmät termit. Tietoevry. Verkkojulkaisu. Viitattu 3.4.2023, 11.4.2023. https://www.tietoevry.com/fi/blogi/2021/05/pilvipalvelut-tieda-tarkeimmat-termit/

Zettler, K. What is cloud computing? An overview of the cloud. Atlassian. Verkkojulkaisu. Viitattu 3.4.2023, 11.4.2023. https://www.atlassian.com/microservices/cloud-computing

Vento, J. 2020. IaaS, CaaS, PaaS, FaaS, SaaS – mitä mikäkin tarkoittaa?. Onrego. Verkkojulkaisu. Viitattu 11.4.2023, 13.4.2023. https://onrego.fi/julkisen-pilven-palvelumallit-avattuna/

What is PaaS? Microsoft Azure. 2023. Verkkojulkaisu. Viitattu 13.4.2023. https://azure.microsoft.com/en-gb/resources/cloud-computing-dictionary/what-is-paas/

Pilvipalveluita käytti 81% yrityksistä vuonna 2022. Tilastokeskus. 2022. Verkkojulkaisu. Viitattu 19.4.2023. https://stat.fi/julkaisu/cktvztyy82z790b55dz6j23q3

Zhang, M. 2023. Top 10 Cloud Service Providers Globally in 2023. Dgtl Infra. Verkkojulkaisu. Viitattu 19.4.2023. https://dgtlinfra.com/top-10-cloud-service-providers-2022/

Barney, N & Gillis, A. 2022. What is public cloud? Everything you need to know. TechTarget. Verkkojulkaisu. Viitattu 19.4.2023. https://www.techtarget.com/searchaws/definition/Amazon-Web-Services

Kurian, T. 2023 The next generation of AI for developers and Google Workspace. Google. Verkkojulkaisu. Viitattu 24.4.2023. https://blog.google/technology/ai/ai-developers-google-cloud-workspace/

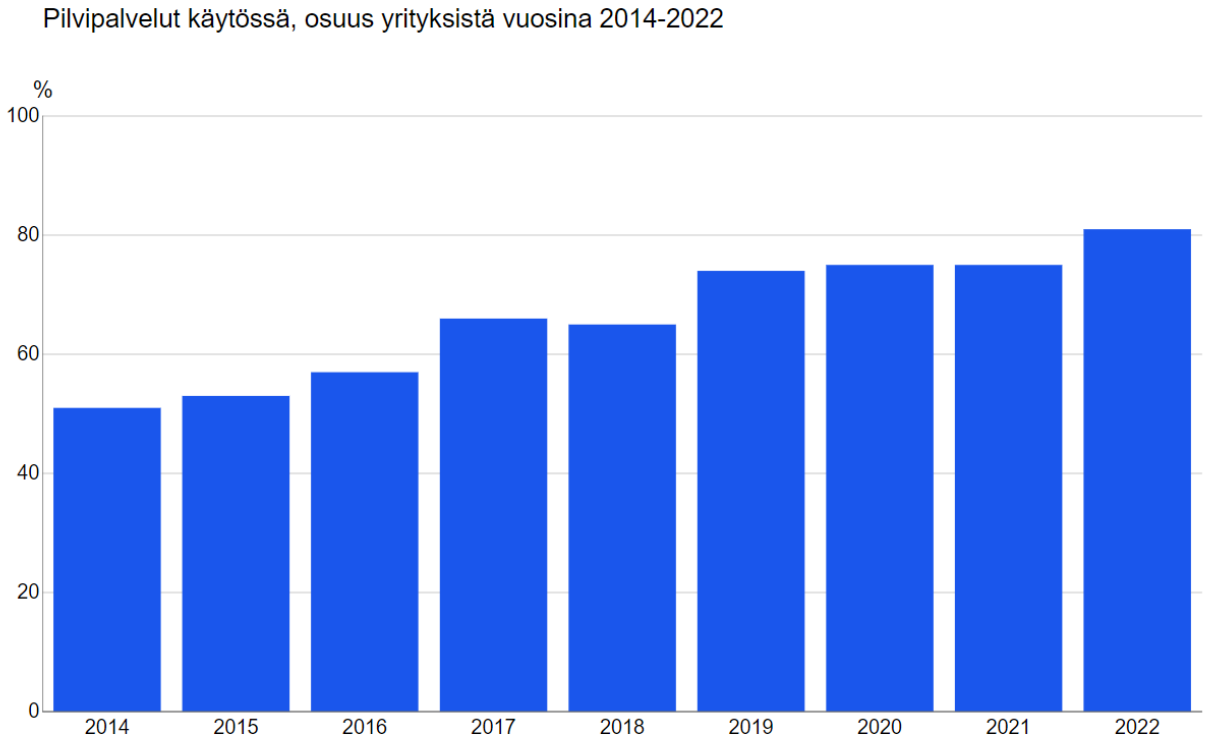
Vetikko, P. 2019. Mikä on ISO 27001 -standardi? Insta. Verkkojulkaisu. Viitattu 24.4.2023. https://www.insta.fi/nakemyksia/tietoturvapalvelut/mika-on-iso-27001-standardi

Pilvipalveluiden turvallisuuden arviointikriteeristö. 2020. Kyberturvallisuuskeskus. PDF-tiedosto. Viitattu 24.4.2023. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Pilvipalveluiden_tietoturva_organisaatioille.pdf

Pilvipalveluiden turvallisuus. 2014. Kyberturvallisuuskeskus. PDF-tiedosto. Viitattu 24.4.2023. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Pilvipalveluiden_tietoturva_organisaatioille.pdf

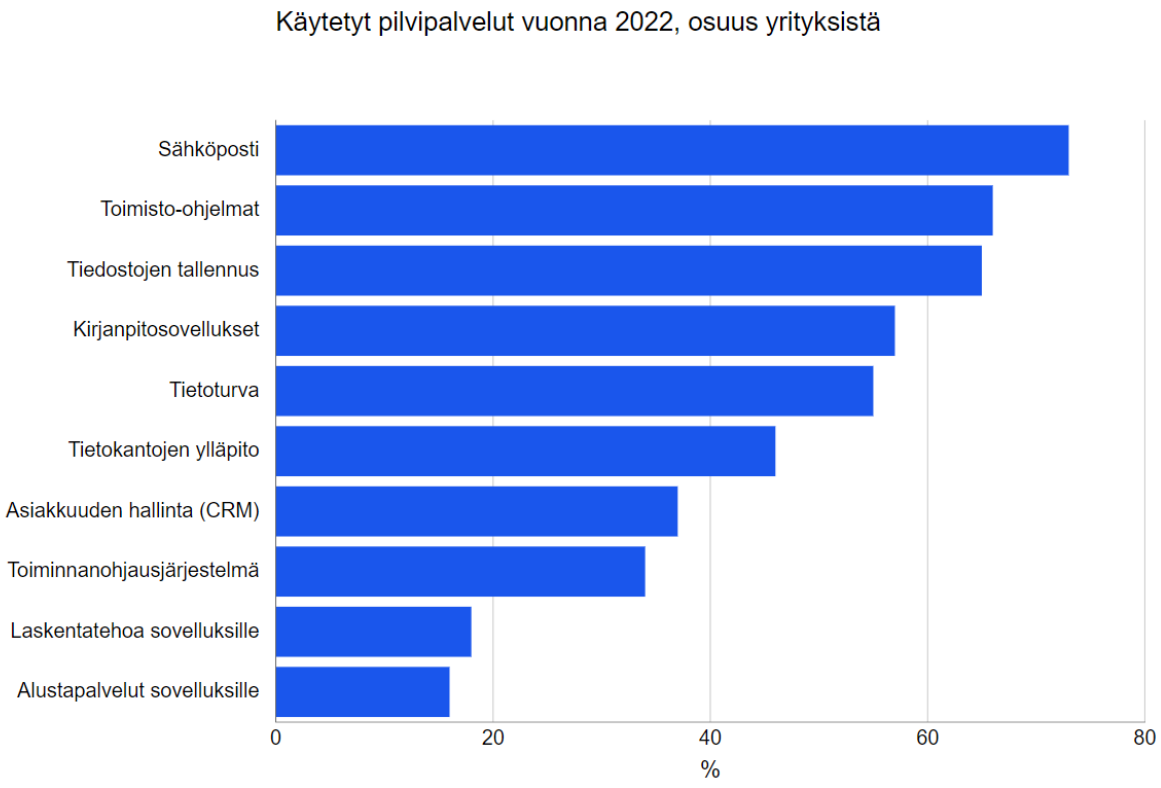
LIITTEET

Liite 1. Pilvipalvelut käytössä, osuus yrityksistä vuosina 2014-2022



Lähde: Tilastokeskus, tietotekniikan käyttö yrityksissä

Liite 2. Käytetyt pilvipalvelut vuonna 2022, osuus yrityksistä



Lähde: Tilastokeskus, tietotekniikan käyttö yrityksissä